WHAT IS CLAIMED IS:

1. A system for securing an application for execution on a computer, the system comprising:

a preprocessor module for identifying calls that are made by the application to at least one routine that is provided by an operating system, the preprocessor module modifying the application such that an interception module is invoked in response to the application invoking the identified routines;

a server computer for receiving at least one application that has been modified by the preprocessor module;

a network; and

a client computer operably connected to the server computer via the network, wherein the client computer receives from the server computer a modified application , wherein subsequent to receiving the application, the client computer executes the modified application.

2. A method of securing an application for execution on a computer, the method comprising:

scanning the application program for code sequences that cause the computer to trap to the operating system;

modifying the code sequences such that the computer does not trap to the operating system;

identifying at least one call that are made by the application to an external routine;

providing at least one interception module for the identified calls;

transmitting the application program and the at least one interception module to the computer;

intercepting at least one of the identified calls at the computer;

monitoring at the computer the usage of resources by the computer; and

preventing the application from consuming resources in excess of a predefined threshold.

3. A method of securing an application for execution on a computer, the method comprising:

scanning the application program for code sequences that cause the computer to trap to the operating system;

modifying the code sequences such that the computer does not trap to the operating system;

identifying at least one call that is made by the application to an external routine;

providing at least one interception module for the identified calls;

transmitting the application program to the computer; and

intercepting at least one of the identified calls at the computer.

4. A method of securing an application for execution on a computer, the method comprising:

identifying calls that are made by the application to an external routine;

modifying the binary of an application to invoke an interception module; and

intercepting at least one of the identified calls at the computer.

5. The method of Claim 4, additionally comprising transmitting the application and at least one interception module to the computer.

6. A method of securing an application for execution on a computer, the method comprising:

identifying calls that cause a detrimental effect to the computer or another application;

modifying a binary of the application to invoke an interception module with respect to the identified calls; and

intercepting at least one of the identified calls.

7. A method of securing an application for execution on a computer, the method comprising:

intercepting at least one call that is made by the application such that a graphical user interface that is displayed by the application is modified;

intercepting at least one call that is made by the application program such that requests for machine or user specific information are virtualized; and

intercepting at least one call that is made by the application such that the contents of at least one file that is used by the application is encrypted transparently to the application.

8. The method of Claim 7, wherein the machine information includes operating system information.

9. The method of Claim 7, additionally comprising intercepting at least one call that is made by the application such that the filename of at least one file that is used by the application is encrypted transparently to the application.

10. The method of Claim 7, additionally comprising modifying a directory structure of a set of files.

11. A method of securing an application for execution on a computer, the method comprising:

intercepting at least one call that is made by the application such that a graphical user interface that is displayed by the application is modified; and

intercepting at least one call that is made by the application such that the contents of at least one file that is used by the application is encrypted transparently to the application.

12. The method of Claim 11, additionally comprising intercepting at least one call that is made by the application such that the filename of at least one file that is used by the application is encrypted transparently to the application.

13. The method of Claim 11, additionally comprising modifying a directory structure of a set of files.

14. A program storage device storing instructions that when executed perform the steps comprising:

intercepting at least one call that is made by the application such that a graphical user interface that is displayed by the application is modified; and

intercepting at least one call that is made by the application such that the contents of at least one file that is used by the application is encrypted transparently to the application.

15. A method for allowing application programs to execute in non-native environments, the method comprising:

identifying a service that is not provided by a selected operating system; and

modifying a binary of an application to invoke an interception service instead of requesting the service from the selected operating system.

16. A program storage device storing instructions that when executed perform the steps comprising:

virtualizing an application interface between a first application and an operating system; and

preventing access by a second application or the operating system to data that is used by the first application.

17. A program storage device storing instructions that when executed perform the steps comprising:

virtualizing an application interface between a first application and an operating system; and

preventing the first application from accessing the second application.

18. A method of securing an application for execution on a computer, the method comprising:

virtualizing an application interface between a first application and an operating system; and

preventing access by a second application or the operating system to data that is used by the first application.

19. The method of Claim 18, additionally comprising restricting access by the application to selected resources on the computer.

20. A system for securing an application for execution on a computer, the system comprising:

means for scanning the application program for code sequences that cause the computer to trap to the operating system;

means for modifying the code sequences such that the computer does not trap to the operating system;

means for identifying calls that are made by the application to an external routine;

means for providing at least one interception module for the identified calls;

means for transmitting the application program and the at least one interception module to the computer;

means for intercepting at least one of the identified calls at the computer;

means for monitoring at the computer the usage of resources by the computer; and

means for preventing the application from consuming resources in excess of a threshold.

21. The system of Claim 20, wherein the threshold is determined in real time by monitoring the system state.

22. A system for securing an application for execution on a computer, the system comprising:

means for scanning the application program for code sequences that cause the computer to trap to the operating system;

means for modifying the code sequences such that the computer does not trap to the operating system;

means for identifying calls that are made by the application to an external routine;

means for providing at least one interception module for the identified calls;

means for transmitting the application program to the computer; and

means for intercepting at least one of the identified calls at the computer.

23. The system of Claim 22, wherein the means for intercepting at least one of the identifies calls prevents the application from communicating with network devices that are not listed in a pre-approved list of network connections.

24. A system for securing an application for execution on a computer, the system comprising:

means for identifying calls that are made by the application to an external routine;

means for providing at least one interception module for the identified calls;

means for transmitting the application program and the interception module to the computer; and

means for intercepting at least one of the identified calls at the computer.

25. A system for securing an application for execution on a computer, the system comprising:

means for intercepting at least one call that is made by the application such that a graphical user interface that is displayed by the application is modified;

means for intercepting at least one call that is made by the application program such that requests for machine or user information are virtualized; and

means for intercepting at least one call that is made by the application such that the contents of at least one file that is used by the application is encrypted transparently to the application.

26. The system of Claim 25, additionally comprising means for intercepting at least one call that is made by the application such that the filename of at least one file that is used by the application is encrypted transparently to the application.

27. The system of Claim 25, additionally comprising means for modifying a directory structure of a set of files.

28. A system for securing an application for execution on a computer, the system comprising:

means for intercepting at least one call that is made by the application such that a graphical user interface that is displayed by the application is modified; and

means for intercepting at least one call that is made by the application such that the contents of at least one file that is used by the application is encrypted transparently to the application.

29. The system of Claim 28, additionally comprising intercepting at least one call that is made by the application such that the filename of at least one file that is used by the application is encrypted transparently to the application.

30. The system of Claim 28, additionally comprising means for modifying a directory structure of a set of files.

31. A system for allowing application programs to execute in non-native environments, the system comprising:

means for identifying a service that is not provided by a selected operating system; and

means for modifying a binary of an application to invoke an interception service instead of requesting the service from the selected operating system.

32. A system for securing an application for execution on a computer, the system comprising:

means for virtualizing an application interface between a first application and an operating system; and

means for preventing access by a second application or operating system to data that is used by the first application.

33. The system of Claim 32, wherein virtualizing the identified calls at the computer comprises virtualizing file system requests.

34. The system of Claim 32, additionally comprising means for restricting access by the application to selected resources on a computer.

35. A system for securing an application for execution on a computer, the system comprising:

a preprocessor module for identifying calls that are made by the application to at least one external routine, the preprocessor module modifying the application to invoke an interception module in response to the application invoking the external routine.

36. The system of Claim 35, wherein the preprocessor module encrypts at least a portion of a filename that is associated with the application.

37. The system of Claim 35, wherein the preprocessor module encrypts the contents of at least a portion of the application.

38. A method of securing an application for execution on a computer, the method comprising:

rewriting the binary of an application thereby preventing the application from: accessing a predefined set of data; invoking a predefined set of instructions; and accessing one or more files that are in one or more predefined directories.

39. The method of Claim 38, additionally comprising rewriting the binary of the application thereby preventing the application from modifying an output device of the computer.